NOMINET CYBER SECURITY

5

Tips on Disrupting the Cyber Kill Chain

IT teams today are faced with a major challenge. The barrier to entry for cyber crime is historically low, with underground sites offering a thriving market in stolen IP and customer data, exploits, hacking tools and even hacker-for-hire services. It's a market said to be worth $1.5tn globally.[1] Attackers are often after lucrative data to steal and sell on, but they could also be looking to conscript corporate machines into botnets which can then be used to spread banking malware, spam, mine illegally for crypto-currency and launch DDoS attacks.

As the cyber criminals become more professional and their attacks more sophisticated, one way for information security teams to approach the challenge has been to use the cyber "kill chain" concept first coined by Lockheed Martin.[2] This breaks down multi-staged network attacks into seven key phases, so that teams can better map security processes and controls to each stage.

- **Reconnaissance:** harvesting email addresses, conference information, etc.
- **Weaponisation:** creating malware that exploits a vulnerability to deliver a payload
- **Delivery:** delivering the weaponised bundle to the victim via email, web, USB, etc.
- **Exploitation:** exploiting a vulnerability to execute code on a victim's system
- **Installation:** installing malware on the asset
- **Command & Control (C2):** command channel for remote manipulation of victim, maintaining persistence
- **Actions on objectives:** with 'Hands on Keyboard' access, intruders accomplish their original goal

By focusing on the DNS, IT teams can disrupt malware at crucial points in the kill chain, most notably at the delivery and C2 stages, regain the initiative and prevent attacks impacting the organisation.

Here are five steps they can take right now:

KILL CHAIN TIPS

TIP 1

Understand the DNS is a weak link in the security chain.

Often referred to as "the phonebook of the internet", DNS is a crucial part of your organisation's internet infrastructure, converting domain names to IP addresses to enable seamless online interactions. Yet it was designed with usability, not security, in mind. This means DNS servers and accounts can be cracked and hacked to alter destination information. Users can then be forwarded to malicious websites, spoofed to appear like legitimate site, but in reality designed to harvest credentials or trigger malware downloads.

[1]Bromium, [2]Lockheed Martin

TIP 2

Prevent the initial exploit.

By focusing their efforts on the DNS, IT and cyber security teams can monitor traffic to prevent the initial exploit/malware delivery point of the cyber kill chain. A user may click on a link in a phishing email, try to visit an infected site in a drive-by-attack, or visit a page hosting malicious advertising. Because their queries to visit these domains are handled by the DNS layer it's a great place to spot evidence of suspicious activity, such as a user being taken to a dubious-looking domain. Find a DNS-based detection and monitoring tool which can stop phishing attacks and malware downloads in this way.

TIP 3

Take steps to disrupt C2 maintenance and persistence.

Another key stage of the kill chain involves the C2 infrastructure. If a corporate client is compromised by malware as above, the attackers will next look to establish access to a domain outside the organisation, one that they control. This will enable them to remotely control the infected machine – potentially downloading additional, more damaging malware such as crypto-mining code, trojans and backdoors. C2 domains are also where stolen data is sent once it is exfiltrated. Sometimes attackers will use domain generating algorithm (DGA) software to ensure their communications aren't disrupted. These programs create new domains on-the-fly, which malware will switch to periodically, making it harder to block malicious activity. The best DNS security tools will be able to spot and disrupt this activity.

TIP 4

Prevent data loss.

The final stage in many attacks is to smuggle stolen data out of the organisation. This theft of data be done at the DNS layer via "tunneling" techniques, which encode small pieces of the stolen data in legitimate-looking queries. Because many firewalls whitelist DNS traffic and the data is well hidden, it can slip under the radar of traditional filters. That's why it's vital for organisations to invest in tools which can spot the tell-tale signs of stolen data leaving the network in unauthorised transfers – whether attackers use off-the-shelf tunneling toolkits or more bespoke techniques.

TIP 5

Find a security partner you can trust.

Finally, remember that not all DNS security solutions are created equal. Proactive visibility and control should be your watchwords. You need a high degree of automation and advanced heuristic capabilities to spot single malicious packets hidden inside vast quantities of legitimate enterprise data. Security platforms must detect and block attacks — disrupting at key points in the cyber kill chain without any hit on performance. Depending on your organisation it may be more appropriate to choose either an on-premises or a managed service solution.

Nominet's Cyber Security Solution – NTX.

NTX will reduce risk on your network and eliminate threats before they cause harm.

All networks rely on DNS traffic. It is a critical source of information to check for threats and monitor the health of a network, but often overlooked in the security stack. NTX analyses network DNS traffic for both known and unknown threats. Embedding our patented algorithms means we eliminate threats from the network and identify zero-day activity not seen by traditional methods of detection. This narrows the window when malicious activity can compromise your network.

Eliminate network threats before they cause harm.

Our continuous R&D efforts create powerful insights to predict, detect and block network threats.

Proven and trusted cyber security services.

Protecting enterprise customers and chosen by UK Government.

Contextualise your network and know what good looks like.

Understand normal network behaviours and identify any abnormal trends.

Threat hunting and forensics.

Granular data capture to provide meaningful insight for the duration of your service.

Easy deployment and integration.

With minimal touchpoints and rich APIs for your existing security investments.

NOMINET

To learn more about our Cyber Security Services, please visit www.nominet.com/cyber